<u>Claims</u>

1.   A method for retrieving digital objects from a group of digital objects maintained by a database, the group of digital objects being represented by the equation $G = \{m_i, i = 1, 2, ..., N\}$, wherein G represents the group of digital objects, N represents the number of digital objects maintained by the database, i represents an index having allowable values between 1 and N inclusive, and m_i represents an ith digital object within the group of digital objects, the method comprising:

generating a random number R and keys k_i, i having allowable values between 1 and N inclusive, for a symmetric key cryptosystem;

determining a prime number p;

encrypting digital object m_i with key k_i using the symmetric key cryptosystem to obtain ciphertext c_i;

assigning a value of $k_i^R \bmod p$ to a key ciphertext s_i;

responsive to the database receiving a request signal from a user, sending c_i and s_i to the user;

receiving from the user a number n of input signals W_j, such that n is less than N, and j is an index having allowable values between 1 and n inclusive;

computing changed ciphertext U_j, such that U_j is equal to $W_j^{1/R \bmod (p-1)} \bmod p$; and

sending U_j to the user.

2.   The method of claim 1, where the modulo operations may be carried out in any group in which a discrete logarithm is infeasible to compute.

1   3.   A method for a user to privately retrieve digital objects from a group of

2 digital objects $G = \{ m_i, i = 1, 2, ..., N\}$ maintained by a database, the method comprising

3 the steps of:

4   sending a request signal to the database;

5   receiving reply signals c_l, s_l, $l = 1, 2, ..., N$ from the database;

6   generating random numbers w_j, computing and sending $W_j = s_{i_j}^{w_j} \bmod p$, $j = 1, 2,$

7   ..., n to the database;

8   receiving signals U_j, $j = 1, 2, ..., n$ from the database;

9   computing $k_{i_j} = Uj^{1/w_j \bmod (p-1)} \bmod p$, $j = 1, 2, ..., n$; and

10   decrypting c_{i_j} with k_{i_j} and a symmetric key cryptosystem to recover digital objects

11   m_{i_j}, $j = 1, 2, ..., n$.

1   4.   The method of claim 3, wherein the modulo operations may be carried out

2 in any group in which a discrete logarithm is infeasible to compute.

1   5.   A method for selectively retrieving digital objects from a database of

2 digital objects using a symmetric key cryptosystem, the method comprising:

3   for each digital object in the database:

4   generating a unique key for the symmetric key cryptosystem;

5   associating the key with the digital object;

6   encrypting the digital object using the associated key and the

7   symmetric key cryptosystem to produce a ciphertext of the

8   digital object;

9   encrypting the associated key to obtain a ciphertext of the key;

10   transmitting the ciphertext of the digital object and the ciphertext of

11   the key associated with the digital object to a user;

12   receiving at least one changed ciphertext of the keys associated with the digital

13   objects in the database;

14   decrypting each received changed ciphertext; and

15   transmitting the decrypted received changed ciphertexts.

16

1   6.   A method for retrieving digital objects from a group of digital objects

2 maintained by a database, the method comprising the steps of:

3   selectively requesting a plurality of digital objects from the database;

4   receiving encrypted ciphertext digital objects from the database;

5   receiving from the database encrypted ciphertext keys associated with the

6   received ciphertext digital objects;

7   encrypting at least one of the encrypted ciphertext keys to obtain changed

8   ciphertext keys;

9   sending the changed ciphertext keys to the database;

10   receiving partially decrypted changed ciphertext keys from the database;

11   decrypting the partially decrypted changed ciphertext keys; and

12   decrypting at least one of the received ciphertext digital objects using the

13   decrypted keys.

1   7.   An apparatus comprising:

2   a computerized database;

3   coupled to the database, a computer user;

4   coupled to the database, a transmitting module for transmitting data to the user;

5   coupled to the database, a receiving module for receiving data from the user;

6   coupled to the database, a random number generating module for generating

7   random numbers;

8   coupled to the database, a key generating module for generating cryptographic

9   keys;

10   coupled to the database, an encrypting module for encrypting data;

11   coupled to the database, a decrypting module for decrypting data;

12   coupled to the user, a requesting module for requesting data from the database;

13   coupled to the user, a transmitting module, for transmitting data to the database;

14   coupled to the user, a receiving module, for receiving data from the database;

15   coupled to the user, a random number generating module for generating random

         numbers;

17   coupled to the user, an encrypting module for encrypting data; and

18   coupled to the user, a decrypting module for decrypting data.

1   8. A computer program product stored on a computer readable medium for

2   retrieving digital objects from a group of digital objects maintained by a database, the

3   computer program product controlling a processor coupled to the medium to perform

4   the operations of:

5   for each digital object in the database:

6   generating a unique key for a symmetric key cryptosystem;

7   associating the key with the digital object;

8   encrypting the digital object using the associated key and the

9   symmetric key cryptosystem to produce a ciphertext of the

10   digital object;

11   encrypting the associated key to obtain a ciphertext of the key;

12   transmitting the ciphertext of the digital object and the ciphertext of

13   the key associated with the digital object to a user;

14   receiving at least one changed ciphertext of the keys associated with the digital

15   objects in the database;

15

16   decrypting each received changed ciphertext; and

17   transmitting the decrypted received changed ciphertexts.